CUSTOMER RELEASE NOTES

Enterasys® C5 Series
Firmware Version 6.41.03.0018
June 2010

INTRODUCTION:

This document provides specific information for version 6.41.03.0018 of firmware for the following C5 products:
Note: this version of firmware is **not compatible** with the Enterasys **C2 or C3** platforms.

C5G124-24	C5G124-24P2	C5G124-48	C5G124-48P2
C5K125-24	C5K125-24P2	C5K125-48	C5K125-48P2
C5K175-24			

Enterasys recommends that you thoroughly review this document prior to installing or upgrading this product.
For the latest firmware versions, visit the Enterasys download site at:
http://secure.enterasys.com/services/support/downloads/software

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	6.41.03.0018	C5 Only Feature Release	June 2010

HARDWARE COMPATIBILITY:

This version of firmware is **not compatible** with the Enterasys **C2 or C3** platforms. This version of firmware is **only supported** on the **C5** switch family.

BOOTPROM COMPATIBILITY:

This version of firmware is compatible with all boot code versions of the Enterasys C5.

NETWORK MANAGEMENT SOFTWARE SUPPORT:

Network Management Suite (NMS)	Version No.
NMS Automated Security Manager	3.3.0
NMS Console	3.3.0
NMS Inventory Manager	3.3.0
NMS Policy Manager	3.3.0
NMS NAC Manager	3.3.0

If you install this image, you may not have control of all the latest features of this product until the next version(s) of network management software. Please review the software release notes for your specific network management platform for details.

PLUGGABLE PORTS SUPPORTED:

MGBICs	Description
MGBIC-LC01	1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550M, LC SFP
MGBIC-LC03	1000Base-SX-LX/LH, MM, 1310 nm Long Wave Length, 2 KM, LC SFP
MGBIC-LC07	Extended 1000Base-LX, IEEE 802.3 SM, 1550 nm Long Wave Length, 110KM, LC SFP
MGBIC-LC09	1000Base-LX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 KM, LC SFP
MGBIC-MT01	1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550 M, MTRJ SFP
MGBIC-02	1000Base-T, IEEE 802.3 Cat5, Copper Twisted Pair, 100 M, RJ45 SFP
MGBIC-08	1000Base-LX/LH, IEEE 802.3 SM, 1550 nm Long Wave Length, 80 KM, LC SFP
MGBIC-LC04	100Base-FX, IEEE 802.3 MM, 1310 nm Long Wave Length, 2 KM, LC SFP
MGBIC-LC05	100Base-FX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 KM, LC SFP
MGBIC-BX10-d	1000Base-BX10-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 10 km, Simplex LC SFP
MGBIC-BX10-u	1000Base-BX10-U Single Fiber SM, Bidirectional 1310nm Tx / 1490nm Rx, 10 km, Simplex LC SFP

The following SFP+ transceivers are supported in the C5K models only:

SFPPs	Description
10GB-ER-SFPP	10 Gb, 10GBASE-ER, IEEE 802.3 SM, 1550 nm Long Wave Length, 40 km, LC SFP+
10GB-LR-SFPP	10 Gb, 10GBASE-LR, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 km, LC SFP+
10GB-LRM-SFPP	10 Gb, 10GBASE-LRM, IEEE 802.3 MM, 1310 nm Long Wave Length, 220 m, LC SFP+
10GB-SR-SFPP	10 Gb, 10GBASE-SR, IEEE 802.3 MM, 850 nm Short Wave Length, 33/82 m, LC SFP+
10GB-C10-SFPP	10 Gb, pluggable copper cable assembly with integrated SFP+ transceivers, 10 meters
10GB-C03-SFPP	10 Gb, pluggable copper cable assembly with integrated SFP+ transceivers, 3 meters
10GB-C01-SFPP	10 Gb, pluggable copper cable assembly with integrated SFP+ transceivers, 1 meter
10GB-LW-SFPP	10Gb, Laserwire® SFP+ adapter for use with Laserwire cable assembly

NOTE: Installing third party or unknown pluggable ports may cause the device to malfunction and will void your warranty.

PRODUCT FEATURES:

What's New in 6.41

More MAC Addresses - 32K MAC addresses are supported in all C5 models.
IEEE 802.3at High Power PoE – Up to 30 watts of PoE power per port.
Redundant Power Supply Options – The C5 PoE RPS can be used in either redundant or additive mode like the G3. Additive mode allows 30 watts of IEEE 802.3at PoE power to be simultaneously delivered to all 48 ports.

Increased Stacking Performance – C5 switches support a 25% increase in performance over the C3. Note that this improved performance requires that new stacking cables be used when stacking C5 swtiches.
No Backwards Stacking – The C5 switches do not stack with the previous generation C-Series products (Enterasys C2 or C3).
Single License for Advanced IPv4 and IPv6 Routing – Separate licenses for advanced multicast IPv4 routing and IPv6 routing no longer exist. One advanced routing license (C5L3-LIC) enables advanced IPv4 multicast routing and IPv6 routing capability.
Greatly Improved Policy Capabilities – More policy users per port (up to 8), more rules per profile (250), more profiles (up to 63) and more rules per switch (up to 3072). See **Policy Capacities for C5 Only** for more details.
Larger Routing Tables – Route table sizes have basically doubled. See **Router Capacities for C5 Only** for details.
100Base-FX Support on All SFP Ports – 100Base-FX transceivers are now supported in every SFP port on the C5 models.
SFP+ Ports with 1Gb and 10Gb Transceiver Support – C5K switches have SFP+ ports that can support either a 1Gb transceiver (MGBIC) or a 10Gb transceiver (SFPP).

Product Features	
Hybrid Policy Mode	VLAN-to-Policy Mapping via hybrid mode
LLDP-MED Network-Policy TLV	sFlow support
TACACS+ management	ACLs per VLAN
Extended ACLs	Host Protect
Secure Copy / Secure FTP (SCP/SFTP)	AES-128 support with SNMPv3
Power Supply & Fan Monitoring via SNMP	Selectable source management interfaces
Copy & Paste of configuration files between switches	RFC3580 dynamic VLAN assignment based on PWA
Multi-user authentication per port (up to 3 policy users per port)	Support for 10GBASE SFP+ transceivers
Multiport LAG to single port LAG automatic failover	100Base-FX MGBIC support in SFP ports
DHCP Spoof Protection	ARP Spoof Protection
IP Forward-Protocol command	High-Temperature Alerts
Control mdi/mdix port settings via CLI to prevent network loops	TDR-based cable status check detects cable breaks and disconnections
Show support command	Configurable Login Banner
Enterasys Policy (role-based L2/L3/L4 access control, QoS, and rate limiting)	48 Gbps Full Duplex (96 Gbps bidirectional) closed-loop stacking
802.1D	32K MAC Address Table
802.1Q - VLAN Tagging	Selectable MAC Hashing Algorithms
802.1p - Traffic Management / Mapping to 6 Queues	Auto-Negotiation
802.3x Flow Control	8 Priority Queues per Port
802.3ad – Dynamic and Static Creation for Link Aggregation (6 LAGs, 8 ports per LAG)	Session-Timeout and Termination-Action RADIUS Attributes Support
802.1s – Multiple Spanning Tree Protocol (up to 4 instances)	Ability to Set Port Advertised Ability via CLI
802.1w – Rapid Spanning Tree	Multi-method Authentication
RFC-3580 dynamic VLAN assignment based on 802.1X or MAC Authentication	Multiple RFC3580 Users per port (up to 8)
Spanning Tree Backup Root	User + IP Phone Authentication

Product Features	
STP Loop Protect	L2 Policy Rules
LLDP/LLDP-MED with TLVs	COS based Inbound Rate Limiter per Policy User
Legacy Path Cost	DHCP Server
STP Pass Through	Web Authentication (PWA)
SpanGuard	Web Redirect – PWA+ and URL redirection
Link Flap Detection	802.1X Authentication
Per Port Broadcast Suppression	Non-Strict 802.1X Default RFC 3580 With Auth Failure
Port Mirroring	RADIUS Client
Protected Port (Private VLAN)	Turn Off RADIUS Authentication (RADIUS Realm)
Cabletron Discovery Protocol (CDP)	Queuing Control Strict and Weighted Round Robin
Cisco Discovery Protocol (CDP) v1/2	MAC Authentication / MAC Authentication Masking
Cisco IP Phone Discovery	MAC Authentication Retained After Age Out
GVRP	RADIUS Accounting for MAC Authentication
IGMP v1/v2/v3 Snooping	EAP Pass Through
Syslog	VLAN marking of mirrored traffic – Edge only
Text-based Configuration Upload/Download	Dynamic and Static MAC Locking
CLI Management	New Mac Trap (like the Matrix-E1)
Telnet Support	Dynamic Egress
IPv4/IPv6 Dual Host Management Support	SSHv2
Discard VLAN Tagged Frames	WebView
Jumbo Frame (up to 9K)	SSL Interface to WebView
Priority Classification L3-L4	RMON (4 groups)
VLAN-to-Policy Mapping on a per Port Basis	RMON View in the CLI With Persistent Sets
Node/Alias Table	RMON Packet Capture/Filtering Sampling
ToS Rewrite	SNMPv1, SNMPv2c, SNMPv3
IPv4/IPv6 Routing	Simple Network Time Protocol (SNTP)
Multiple IP Helpers per Interface (up to 6)	Alias Port Naming
ACLs	Ability to Set Time and Date via the MIB
IPv4 Routing Protocols: RIP, OSPF, VRRP, DVMRP, IRDP, PIM-SM	CoS MIB based Flood Control (broadcast, multicast, and unknown unicast)
IPv6 Routing Protocols: OSPFv3	CPU/Memory utilization monitoring via SNMP
IPV6 Tunneling	SMON MIB support for Port Mirroring

INSTALLATION AND CONFIGURATION NOTES:

Note:
As a best practice, Enterasys recommends that prior to upgrading the firmware on your switch, you save the existing working configuration of the system by using the **show config outfile** configs/<*filename*> command.

Please go to http://www.enterasys.com/download/download.cgi?lib=c5 for the latest firmware updates for the C5 Series. If you would like to upgrade an existing C5, follow the TFTP download instructions that are included in your CLI Reference or use NMS Inventory Manager to upgrade the switch.

TFTP download instructions are also available under the Hot Topics list on the Enterasys support web site at: https://knowledgebase-enterasys.talismaonline.com

Soft copies of the C5 CLI Reference are available at no cost on the Enterasys Networks web site, http://secure.enterasys.com/support/manuals/

The C5 Series of stackable switches is managed by a single IP address for a stack of up to 8 switches.

In order to download the new software to a stack of C5 switches, simply follow the instructions to upgrade a switch with new software. The system will then automatically download the new software to all the members in the stack controlled by that stack manager.

Policy Capacities for C5 Only

Feature	Capacity
Policy roles (profiles) per system	63
Number of users per port	Tunnel Mode = 8, Policy Mode = 8, Hybrid Mode = 8
Number of unique rules per system	3072
L3/L4 rules	2048
EtherType rules	512
MAC rules	512
Number of rules per single role	250
Number of masks	No Limit
COS rate limiting (IRL)	Yes
Role-based rate limiting	Yes
Rule-based rate limiting	No
Priority-based rate limiting	No
Fixed rule precedence	Yes
VLAN to policy mapping**	Assign VLAN traffic to use a specific policy
Rule Types	
EtherType*	VLAN/cos/drop/forward***
MAC dest / MAC source	Cos/drop/forward
IP Protocol	Cos/drop/forward
IP dest socket / IP source socket	Cos/drop/forward
IP TOS	Cos/drop/forward
TCP dest port / TCP source port	Cos/drop/forward
UDP dest port / UDP source port	Cos/drop/forward
ICMP Type	No

* The EtherType to VLAN mapping rule is supported only when ‘numusers’ (number of users allowed to authenticate on a port) is set to 1.

** The VLAN to policy mapping rule is supported only when ‘numusers’ (number of users allowed to authenticate on a port) is set to 2 or greater.

*** When configuring EtherType to VLAN rules, there is a maximum of 7 VLAN rules per profile.

Router Capacities for C5 Only

Feature	Capacity
ARP Dynamic	4048
ARP Static	1024
IPv4 Route Table	5000
IPv6 Route Table	3000
OSPF Areas	8
Total OSPF LSA Type	5000
OSPF LSA Type 1 – Router Links	No restriction can equal 5000
OSPF LSA Type 2 – Networks Links	No restriction can equal 5000
OSPF LSA Type 3 – Summary Networks	No restriction can equal 5000
OSPF LSA Type 4 – Summary ASBRs	No restriction can equal 5000
OSPF LSA Type 5 – AS External Links	No restriction can equal 5000
OSPF LSA Type 7 – NSSA External Links	No restriction can equal 5000
OSPF LSA Type 9 – Opaque Subnet-only	Not Supported
OSPF LSA Type 10 – Opaque Area	Not Supported
OSPF LSA Type 11 – Opaque AS	Not Supported
OSPF ECMP Paths	4
Static Routes	128
RIP Routes	5000
IP Interfaces	48
Secondary Interfaces	62
VRRP Interfaces	20
IP Helper Address	6 per interface
Access Rules (inbound only)	400
Access Rules – Per ACL	80 per list – 240 total per interface
Multicast Groups	1024
DVMRP Routes	512

sFlow Capacities

Feature	Capacity
Number of sFlow pollers	unlimited
Number of sFlow samplers	32

FIRMWARE CHANGES AND ENHANCEMENTS:

Initial firmware release for C5 switching products.

KNOWN RESTRICTIONS AND LIMITATIONS:

Warning:
MGBIC-LC04 and MGBIC-LC05 are only supported in standalone units. If you install them on stack member units, loss of link may result.

1 Gigabit SFPs are only supported in SFP+ ports on standalone units. If you install them in stack member units, loss of link may result.

Known Issues in 6.41.03.0018
Switching
COS / TOS
13257 When the C5 is configured for “User + Phone” authentication, the phone’s VLAN-tag to role mapping will be counted as a user against the number of multiauth users allowed per-port.
2731 If the CoS state is disabled, but a CoS priority has been configured, the switch will continue to forward packets with the CoS priority. However, the ToS field will not be modified.
6660 Configuring the last two bits of the ToS field is not supported. For example, when a CoS Index is configured to set a ToS value of 255, it will result in only the value 0xFC being set in the matching packets.
Dynamic Egress
Egress assignments made to ports by using Dynamic Egress are only supported on VLANs which have been statically created.
GVRP
13946 GVRP will not automatically propagate VLANs assigned to ports via vlan authentication. The workaround is to manually add egress to the uplink port.
3532 GVRP frames are not forwarded when GVRP is disabled.
2031 The switch will propagate GVRP packets containing any known VLANs. All VLANs learned via GVRP will appear in the GVRP MIBs, regardless of whether or not there are local users attached to those VLANs.
LACP
9700 The output of the CLI command “show port lacp port <port-string> status detail” does not reflect the correct partner values for the ActorAdminKey and ActorOperKey.
Linkflap
6851 Link Flap Detection cannot be configured on a port that is a member of a link aggregation group (LAG).
VLAN Tagging
3272 VLAN ID 4094 is not supported and is reserved for other use in the system.
3410 The “set port vlan” command requires that the VLAN(s) specified when executing the command must already be preconfigured statically on the device.
A VLAN cannot be disabled via CLI and/or WebView. SNMP must be used.

Known Issues in 6.41.03.0018
Policy / Authentication
13770 When running multiple authentication mechanisms dot1x and macauth, dot1x should have higher precedence. If the order is reversed, dot1x authenticated traffic is diverted to the host until macauth is performed.
13998 When setting the multiauth mode from multi to strict, some previously authenticated users may be unable to re-authenticate. The work around is to disable PWA and MAC Authentication prior to switching modes.
TACACS+ using single connect is configurable through the CLI but it is not supported in this release.
The C5 supports CoS-based Inbound Rate Limits for Policy Roles (profiles). Rule-based Inbound Rate Limits (IRLs) are not supported and will be ignored if configured.
Setting an extensive number of policy rules via the CLI can cause momentary loss of CLI and SNMP management.
Policies can only be assigned to ports on VLANs which have been statically created.
Policy roles and rules cannot be applied to ports that are members of a link aggregation group (LAG).
3904 If a policy profile has CoS-status enabled, only 249 rules can be supported per policy profile.
2175 ARP packets are not classified based on policy IP source/destination rules.
MAC Locking
Static MAC locking a user on multiple ports is not supported.
A violating MAC lock user can authenticate on the port using dot1x, but all other traffic from that user will be dropped.
Statically MAC locked addresses in the Filtering Database show as “other” in the “show mac” response.
The MAC lock table may show multiple entries for the same user depending upon the VLAN assignment.
RADIUS
By design, the switch does not allow the Primary and Secondary RADIUS servers to use the same IP address.
MAC Authentication
10893 There is a potential for the MAC address of a user who fails to authenticate to remain unlearned for a period of time.
In some rare cases, the command “set macauthentication portinitialize <port-string>” does not terminate mac-authenticated user sessions.
PWA
13849 When PWA enhanced mode is enabled and a user authenticates with a lower precedence method, that user’s port 80 traffic will continue to be intercepted, until PWA authenticates the user. The work around to this is to ensure PWA has a lesser precedence.
On switches that support multiauth, only one PWA authenticated user is supported per port

Spanning Tree
The “show spantree stats active” command may erroneously display some ports as active. If a port was once active and later goes down, the system will still show the port on the “active” list.
VLAN marking of mirrored traffic – Edge only
MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.

Warning: Traffic mirrored to a VLAN may contain control traffic. This may be interpreted by the downstream neighbor as legal control frames. Users should disable any protocols on inter-switch connections that might be affected (for example, Spanning Tree).
Routing
You cannot overwrite the IP address of a configured interface if the new IP address is in the same subnet as the original. You must first delete the existing interface IP address and then add the new IP address.
The C5 will not add a dynamic host route to its routing table for a subnet it already knows about.
The C5 does not support configuring the host's gateway to be a local routed interface IP. The host's gateway must exist on a different device in the network, if one is configured.
The C5 only supports one default route. If a default route is configured on the router, it will take precedence over the default route configured for the host IP.
ACLs
You can apply an ACL to a routed VLAN interface or a policy to a port. However, the device does not support enabling both features simultaneously on a port that is part of a routed VLAN interface.
IPv6
14036 When using IPv6 management, the movement of the master as the result of a "set switch movemanagement" commands or a reset, can result in the loss of the host address. This can result in the loss of remote management. This can only be recovered by reloading the configuration.
Servers for RADIUS, Syslog, PWA, or SNTP cannot be configured with an IPv6 address.
OSPFv3 virtual links are not displayed in the OSPF adjacency table.
RIP
If a secondary address is added to an interface advertising RIPv2 via the "redistribute connect" command, the router will send an initial RIP response packet which includes the secondary address. But in subsequent updates, the route is not advertised.
RIP stops calculating cost properly if cost ever equaled 16. If route cost is reduced below 16, the cost will not be propagated downstream properly.
14132 RIP md5 authentication has an invalid format. Workaround: Do not use md5 authentication for RIP.
OSPFv2
OSPF area 0 is always configured by default on the C5.
The OSPF ABR doesn't insert the default route into the NSSA when using the command "area <area_id> nssa". The default does get inserted when using the command "area <area_id> nssa default-information-originate".
The C5 only redistributes inter-area and intra-area OSPF routes via RIP. The redistribution of external type 1, external type 2, NSSA, and stub routes into RIP is not supported.
Area default-cost parameter isn't used when the ABR router is configured for an NSSA.
The C5 does not redistribute the default route via OSPF redistribution.
When creating a stub or NSSA area, in order to remove the existing summary or external LSAs before they age out naturally, all of the stub/NSSA area routers can either be reset, or the user can stop and restart the OSPF process. Otherwise, after 3600 seconds have passed, the MaxAged Summary or External LSAs will be removed automatically.

Multicast Routing
The output of "show ip mroute" will display the source mask address as 0.0.0.0.
The mroute table source network field displays the host IP address, not the host network.

Management
The switch can support up to two concurrent SSH client sessions.
9328 If the host IP address or the router IP interface used for management is in a zero subnet (for example, 10.0.x.x/16), ARPs will resolve, and the host will be unable to ping devices within the subnet.
9367 ICMP packets containing the record route or timestamp options will not be forwarded by the device.
11539 It is highly recommended that DAI (dynamic ARP inspection) be configured on edge ports only, due to the potential for the DHCP snooping database to become out of sync during a system reset.
11593 Setting the SNMP community context to default via the “set snmp community xxx context default” command could cause loss of SNMP management contact. In order to set a configured context back to the default (NULL) context, enter a hyphen as the value of the context parameter. For example, use the following command: “set snmp community abcde context –”.
12329 You cannot set port advertise speeds of 10t, 10tfd, 100tx, and 100txfd on combo ports.
12737 When initiating a telnet session from the console of the device to another device, the telnet session will occasionally fail with the following error message: “telnet: Unable to connect to remote host: Connection timed out”. Executing the command a second time will succeed.
13709 Auto-negotiation is required for MGBIC-LC01 link.
13972 Link Traps will only be sent to a maximum of three SNMPv3 notification targets.
14129 Disabling flow control while the system is under load may cause ports to stop forwarding. If it is desired to have flow control disabled, it is recommended that the switch be preconfigured.
WebView (Web-based Management)
Configuration information for LAGs configured via WebView will not be reflected correctly when viewed via the CLI.
RMON
When packets are transmitted outbound, they are counted under packet sizes 64 -1518 in RMON stats but not total Packets or Octets.
Enabling RMON capture on an interface will cause packets to be duplicated on the interface while the functionality is enabled.
Only RMON offset values of 1 through 1518 are supported.
RMON automatically creates entries for stats using indexes associated with each port. If any of the automatically created indexes are cleared and then associated with a new entry with an index less than 450, the new entries will not be persistent. Upon resetting the device, RMON will automatically create entries for each port using the initial default indexes. To avoid this situation, always use an index of 450 or greater when creating new entries.
Port counters and RMON counters may display differing values.
Packets greater than 1518 will not be counted by the IfInErrors MIB.
sFlow
14061 sFlow can create varying degrees of CPU utilization depending on the number of samplers, sampling rate, pollers, and sampling interval. High CPU utilization can be mitigated by reducing samplers and pollers, or increasing sampling rate and interval. Since traffic is switched in hardware, CPU utilization should not affect switch performance. However, it may slow management response.
12004 sFlow does not sample with frame rates less than 1024fps.

For the most up-to-date information concerning known issues, go to the **Global Knowledgebase** section at http://www.enterasys.com/support/.

For the latest copy of this release notes, go to http://www.enterasys.com/services/support/downloads/.

To report an issue not listed in this document or in the **Global Knowledgebase**, contact our Technical Support Staff.

IETF STANDARDS MIB SUPPORT:

RFC No.	Title
RFC 1213	MIBII
RFC 1493	Bridge MIB
RFC 2613	SMON MIB (portCopyConfig)
RFC 2819	RMON MIB
RFC 2668	Ethernet-Like MIB
RFC 2233	IfMIB
RFC 2863	IfMIB
RFC 2620	Radius Accounting MIB
RFC 2618	Radius Authentication MIB
RFC 3621	Power Ethernet MIB
IEEE 802.1X MIB	802.1-PAE-MIB
IEEE 802.3ad MIB	IEEE 8023-LAG-MIB
RFC 2674	802.1p/Q BridgeMIB
RFC 2737	Entity MIB (physical branch only)
RFC 2933	IGMP MIB
RFC 2271	SNMP Framework MIB
RFC 3413	SNMP Applications MIB
RFC 3414	SNMP Usm MIB
RFC 3415	SNMP Vacm MIB
RFC 3584	SNMP Community MIB
RFC 1248	OSPF Version 2 MIB
RFC 1724	RIP Version 2 MIB
RFC 2787	VRRP MIB
RFC 1981	Path MTU for IPv6
RFC 2465	IPv6 MIB
RFC 2466	ICMPv6 MIB

ENTERASYS NETWORKS PRIVATE ENTERPRISE MIB SUPPORT:

Title
ctbroadcast mib
ctenvironment mib
ctRatePolicing mib
ctQBridgeMIBExt mib
ctCDP mib
ctAliasMib
ctTxQArb mib
ctDownLoad mib
ctEntStateOperEnabled and ctEntStateOperDisabled
etsysRadiusAuthClientMIB
etsysRadiusAuthClientEncryptMIB
etsysPolicyProfileMIB
etsysPwaMIB

Title
etsysSyslogClientMIB
etsysConfigurationManagementMIB
etsysMACLockingMIB
etsysSnmpPersistenceMIB
etsysMstpMIB
etsysMACAuthenticationMIB
etsysletfBridgeMibExtMIB
etsysMultiAuthMIB
etsysSntpClientMIB
etsysIeee8023LagMibExtMIB
etsysVlanAuthorizationMIB
etsysCosMIB
etsysResourceUtilizationMIB
etsysMultiUser8021xMIB
etsysTacacsClientMIB

Enterasys Networks Private Enterprise MIBs are available in ASN.1 format from the Enterasys Networks web site at: http://www.enterasys.com/support/mibs/ . Indexed MIB documentation is also available.

SNMP TRAP SUPPORT:

Traps	Description
Authentication Failure	User has failed network authentication
ColdStart (RFC 1213)	System has initialized due to power-up
CPU Utilization	CPU utilization exceeds configured threshold
ctEntStateOperEnabled	Unit has joined the stack
ctEntStateOperDisabled	Unit has left the stack
etsysPsePowerNotification	Power system failure
Fan failure	Fan state transitioned from “normal to failing” or from “failing to normal”
Link Up (RFC 1213)	User port transitioned to an up state
Link Down (RFC 1213)	User port transitioned to an up state
Link Flap	Link pattern has exceeded threshold parameters
LLDP	Remote system change detected
LLDP-MED	Topology change detected on the port (that is remote device has been attached or removed from the port)
newaddrtrap	New MAC address detected on non-CDP port
Maclock violation	Detected source MAC address not permitted
Overtemperature	Transitioned to thermal alarm state
PoE inlinepower	Port status change or power threshold exceeded
Policy Inbound Rate Limit	Rate limit violation
RMON FallingAlarm (RFC 1757)	A monitored MIB decreased to a trigger value
RMON RisingAlarm (RFC 1757)	A monitored MIB increased to a trigger value
RPS Power status	Redundant Power Supply status change
STP Disputed BPDU	Disputed BPDU events exceeded threshold
STP Loop Protect	Inconsistent BPDU receipt on ISL port
STP New Root (RFC 1493)	Root bridge role transition has occurred
STP Spanguard	Incoming BPDU detected on edge port
STP Topology Change (RFC 1493)	Spanning Tree topology has changed

RADIUS ATTRIBUTES SUPPORT:

Attribute	RFC Source
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579
Filter-ID	RFC 2865, RFC 3580
Framed-MTU	RFC 2865, RFC 3580
Message-Authenticator	RFC 3579
NAS-Identifier	RFC 2865, RFC 3580
NAS-IP-Address	RFC 2865, RFC 3580
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-Type	RFC 2865, RFC 3580
Session-Timeout	RFC 2865
State	RFC 2865
Termination-Action	RFC 2865, RFC 3580
Tunnel Attributes	RFC 2867, RFC 2868, RFC 3580
User-Name	RFC 2865, RFC 3580

RADIUS Accounting Attributes

Attribute	RFC Source
Acct-Session-Id	RFC 2866
Acct-Terminate-Cause	RFC 2866

GLOBAL SUPPORT:

By Phone: 978-684-1000
1-800-872-8440 (toll-free in U.S. and Canada)

For the Enterasys Networks Support toll-free number in your country:
http://www.enterasys.com/support/

By Email: support@enterasys.com

By Web: http://www.enterasys.com/support/

By Mail: Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810 (USA)

For information regarding the latest software available, recent release notes revisions, or if you require additional assistance, please visit the Enterasys Networks Support web site.